Departments of Defense and Veterans Affairs (DOD/VA) integrated Electronic Health Record (iEHR)

Technical Specifications Summary

Version 1.6

July 31, 2012

IPO
INTERAGENCY
PROGRAM OFFICE

TABLE OF CONTENTS

Table of Appendices

Document Approval

****

CONCURRED BY:

Name
Title
Organization

DATE

Name
Title
Organization

DATE

Name
Title
Organization

DATE

Name
Title
Organization

DATE

****

Disclaimer

The information in this DRAFT document is believed to be accurate and reliable. The origin of this information may be internal or external to the Departments of Defense and Veterans Affairs (DOD/VA) and the jointly-managed Interagency Program Office (IPO). IPO staff has made all reasonable efforts to verify the information in this document.

Document Change Control

Version	Date	Brief Description of Changes
1.2	May 16, 2012	Formatting, added language, basic editing
1.3	May 21, 2012	Updated with GC-Mr. Rosen's change's, updated Capability descriptions, other minor changes
1.4	May 25, 2012	Final edits for Pharm RFI RFK
1.5	May 30, 2012	Moved artifact listing to Appendix, updated Appendix with Alpha vs. Roman Numeral
1.6	July 31, 2012	Updated entire document – inclusion of IPO document template, addition of content to satisfy unintended gaps/omissions, additional Appendix A for reference documents

1.0 Introduction

1.1 Background

The Department of Defense (DoD) and the Department of Veterans Affairs (VA) operate two of the nation's largest health care systems, providing health care to service members and veterans at estimated annual costs of about $49 billion and $48 billion, respectively. To do so, both departments rely on electronic health record systems to create, maintain, and manage patient health information.

In January 2008, The VA and DoD received a report documenting that 97 percent commonality of iEHR requirements between both departments while only 3 percent were Department specific. As a result, VA and DoD began to examine the possibility of jointly developing an iEHR and system. By February 2011, the Deputy Secretary of Veteran Affairs, the Deputy Secretary of Defense, and the Vice Chairman of the Joint Chief of Staff agreed to an approach for a joint VA–DoD iEHR, formally establishing the Interagency Program Office (IPO) in support of the following joint goals:

- Improve the quality and accessibility of health care, benefits, and memorial services while optimizing value
- Optimize workflow for healthcare providers Increase service member and veteran satisfaction

Key to establishing a joint iEHR, including improvement of quality of care while conserving resources through identifying and utilizing commonality, is the establishment of a robust infrastructure. Loosely defined as the information technology components that will enable the delivery of new clinical capabilities to the end user, the iEHR infrastructure capability set will enable the effective, efficient delivery of capabilities while leveraging a shared services Service Oriented Architecture (SOA) paradigm.

1.2 Agile Transformation

The DoD/VA Interagency Program Office (IPO) is undergoing agile transformation that will enable it to create value, be flexible, remain in balance, and adapt while serving customers and responding to constant global and technological changes within the Health IT environment. Part of this transformation will include implementation of the Scrum process, which involves project teams acting as self-directed entities composed of Scrum Masters from a cross section of the DoD/VA IPO workforce. Members serve as facilitators to their assigned manager (a.k.a. Product Owner) and are tasked with providing assistance supporting the implementation of program management, software development, business operations, etc. (i.e. scrum) within the enterprise. During this transition, the IPO will stand up an Enterprise Transition Community (ETC) – a small group that initiates, encourages, and supports an organization's effort to introduce and improve through Scrum – in order to realize the following mission, vision and goals:

Mission

Assist DoD/VA IPO managers/sponsors in more effectively planning and implementing a gated agile approach to transforming the delivery of healthcare solutions to the Departments.

Vision

The successful implementation of an agile development and management methodology through the use of Scrum to achieve and/or exceed established financial, schedule, performance and human capital goals.

Goals

- Increase awareness and commitment to accelerated delivery of improved capabilities to customers
- Expand the use of agile principles and processes to the maximum extent practicable on projects/sprints
- Increase the value added and effectiveness of collaboration efforts by sharing successes and lessons learned
- Achieve a higher return on investment by implementing sprints faster, cheaper and more effectively

1.3 Purpose of the Document

The purpose of this Technical Specifications Summary document is to offer potential support providers / future vendors with an overview of the technical specifications and requirements that define the needs for a standardized, interoperable, future state iEHR environment. The combination of this document and the associated artifacts referenced in APPENDIX B: makes up the iEHR Technical Specifications Package, which will be included as part of each Request for Information (RFI) / Request for Proposal (RFP) released from the Interagency Program Office (IPO) where vendors would require detailed technical specifications and understanding of the iEHR technical environment (as-is and to-be).

1.4 Changes and Revisions

This Technical Specifications Summary document and its associated artifacts are considered a living Technical Specifications Package and may change. Included content and artifacts are intended to represent a joint DoD/VA end-state vision but may still be department specific in the early stages of this initiative. Revisions and updates are made as the iEHR program matures.

1.5 Representative Artifacts

Representative artifacts available at ***www.tricare.mil/iEHR*** then click on Vendor Information in the left column.

2.0 iEHR Enterprise Architecture

The iEHR architecture is comprised of an integrated set of target-state information that provides technical direction for the overall iEHR effort, including future DoD, VA, and integrated DoD-VA iEHR programs, projects, and initiatives. It includes information and models that reflect and support both current and future high-level decisions related to DoD and VA iEHR efforts. Additionally, this comprehensive and integrated iEHR enterprise architecture provides the context for managing the complexity of the existing iEHR environment and the many projects that will maintain and transform the DoD and VA iEHR enterprises.

2.1 Architecture and Standards Compliance Criteria

The architecture and standards compliance criteria worksheets provide an organized, diverse view of the different requirements put forth by the government in support of future technical and functional capabilities. The document includes technical specifications, non-functional/information technology requirements, and certain functional/business specific requirements which capture necessary activities and parameters required for the analysis, and acquisition of an iEHR increment or capability. The architecture and standards compliance criteria incorporates the items necessary for a meaningful analysis and procurement, to serve as a reference working model and unified framework. These worksheets will be provided to a potential vendor as a component of the solicitation process. Prospective iEHR vendors will then be asked to populate and return the worksheet(s) as a portion of their response for government review and evaluation.

2.2 Open Application Programming Interface (API)'s and Common Interface Standards

For Commercial off the Shelf (COTS) products that are being implemented, the contractor shall provide, "fit for purpose," DoD Architecture Framework (DoDAF) artifacts, if available; or, other architecture artifacts describing the integration of the product into the Military Health System (MHS) environment as well as viewpoints describing any custom extensions. (The COTS vendor shall continue to provide architectural documents or instructions that accompany the COTS product package).

The contractor shall conform to the current version of the iEHR Standards Profile (StdV-1) and Standards Forecast (StdV-2), which includes the iEHR health data standards.

The contractor shall, at a minimum, deliver and demonstrate SOA capabilities of the system with the following measures and attributes if applicable:

- Use secure web services that account for multiple technologies and protocols such as service queues and brokers using access control lists and as described in National Institute of Standards and Technology (NIST) Special Publication 800-95, *Guide to Secure Web Services*
- Demonstrate global error handling processes to ensure errors are captured in one central location
- Use IPO iEHR security practices, protocols, and technologies
- Service contracts and Interfaces shall conform to Service Oriented Enterprise (SOE) standards (when available) and metadata shall conform to iEHR metadata inventory guidelines (when available) to allow for querying through a Universal Description Discovery and Integration
- All services developed as part of this solution shall be built using a business process definition and iEHR-specific standards and criteria detailed within the current iEHR EA StdV-1, StdV-2 state iEHR IT platforms

- Services shall be testable, loosely coupled, and support deployment on as-is and future state iEHR Information Technology (IT) platforms
- Services and the SOA Suite will support multiple messaging technology protocols such as messaging queues
- Services shall be implemented to support Web Services Interoperability (WS-I) standards (e.g., Web Services-Business Process Execution Language (WS-BPEL), WS-Security) with additional integration of systems (e.g., a business process engine) into the architecture
- Services shall minimally accept Simple Object Access Protocol (SOAP) messages and support the ability to add text files and other Multipurpose Internet Mail Extensions (MIME) type to the message payload
- The service specification for a SOA service shall be clearly described and accompany the code which includes, but is not limited to, interface documents (i.e., Web Services Description Language (WSDL), security constraints, impact of running multiple versions of a service, and functional and non-functional requirements associated with the service
- A context map shall describe service orchestration, mediation of services and the linking of services to existing systems or operational functions
- Extensible Markup Language (XML) schema shall be delineated so that producers and consumers can use the same schema definition
- The contractor shall document the metadata identified for submission to the iEHR Federated Data Repository (FDR) in accordance with guidance and criteria provided within the standard enterprise architecture requirements for acquiring information management/IT products and services, as required
- The contractor shall submit the metadata to the IPO chief architect for compliance review and approval by the data manager
- Once the submitted metadata has been approved by the IPO chief architect, the contractor may be requested to enter the approved metadata into the appropriate iEHR approved submission package
- Metadata will be tagged as XML, XML Schema Definition (XSD), etc., according to iEHR requirements
- The contractor shall leverage all available and suitable common services and code components from the Common Development Library (CDL)/service development tool kit as part of the solution design and final product delivery
- The contractor shall create software that is platform agnostic, using open standards if applicable

3.0 Enabling Infrastructure Capabilities

3.1 Access

Access Control

The access control capability safeguards and manages individuals' personal and health information. The access control access and authorization capabilities ensure that people, computer systems, and software applications can use only those resources (e.g., files, directories, computers, networks) in an Electronic Health Record (EHR) system of systems that they are authorized to use at the right time and then only for approved purposes. Access controls protect against unauthorized use, disclosure, modification, and destruction of resources and unauthorized issuing of system commands.

The access control capability identifies patients, clinical and administrative users in an EHR system. The access control capability controls access by these users to protected health data and information resources in the EHR system based upon purpose of use, established rules and security policy. Access control mechanisms can be identity, context, role, attribute, or rule-based.

The access control capability involves properly identifying clinical organizations, departments, patients, health employees, and care providers and authorizing their access to health information systems and networks. This enables the sharing of subsets of information with certain customers, vendors, and partners as needed, such that the information available can be adapted to particular users or groups. Care teams will be able to access results and output from ancillary services, enabling the flow and accessibility (across multiple sites) of standardized information within the integrated DoD and VA system.

The access control capability involves properly identifying health information attributes that may be used to restrict access based upon clinical information categories and tagging. This enables the sharing of subsets of information with customers, vendors and partners as needed based upon data segmentation.

The access control capability authenticates users and grants or denies access to protected health information based upon user role-profile attributes, access authorization levels and system access rules. This information includes beneficiaries' medical history, test and laboratory results, insurance information, demographic information, and other data. Access control rules are based upon a combination of patient requests, Federal law, and DoD/VA security policy as well as context constraints.

The access control capability includes the functions of a single sign-on application, which verifies users' credentials once in a session but thereafter provides access to multiple applications.

The access control capability includes the ability for patients to electronically sign documents regarding the sharing of their information and to whom as permitted by policy and law. Typically a patient has the right to view his or her EHR and the right to place restrictions on who can view a part or the whole of that EHR. Such requests include but are not limited to HIPAA authorizations, revocations, restrictions and right of access requests.

The access control capability includes functions to ensure user accountability. The accountability control objective is stated as: "Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked." Accountability is the concept that individual persons or entities can be held responsible for their actions, such as breaching confidentiality. Accountability is achieved through the implementation of a pervasive technical audit service. Audit provides a record of potential insecurities irrefutably traceable back to the originator of the action. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to assess and evaluate the accountability information by a secure means, within a reasonable amount of time and without undue difficulty.

Access Management

Access management is that portion of access control specifically involved with granting of access rights, the management of access control decision information and the definition and management of security policy (rules) required for controlled access to healthcare information. It provides the ability to create and update sets of access control permissions granted to specific users. Access control and authorization mechanisms can be identity, context, role, attribute, or rule-based.

The access control capability also includes an organization's ability to manage a patient's potential to view his or her Electronic health record (EHR) based on scope of practice, organization policy, or jurisdictional law. Typically, a patient has the right to view his or her EHR and the right to place restrictions on who can view a part or the whole of that EHR. Views of the information are tailored to the user's security level and access need.

Access management requires an integrated approach to access management that provides the infrastructure to meet the following needs:

- To consistently authenticate users across enterprise and extranet/federated boundaries
- To consistently authorize/grant users permissions to protected VA information assets
- To robustly enforce access to protected VA information assets
- To audit access to and use of sensitive information and functions
- To meet Federal guidelines and mandates for information security

Access control decision information includes:

- Requester information including identity, role(s), and security attribute, organization, location
- System information attributes (tags)
- Provider information (attributes) such as any credentials, certifications or any other information that may be used to verify that a practitioner is permitted to use or access authorized data including attributes
- Contextual information (e.g. purpose of use, the number of users in a specific role, separation of duty, time and location constraints)

Authorization

Authorization management identifies and manages the access privileges granted to a user, program, or process. Authorization management is the process of granting a person the authorization to perform certain workflow tasks/activities requiring access to various areas, assets, or system-related items by simple decree or by being given a title or moved into a role defined by those tasks. The person will generally not be able to perform the tasks, unless they possess access privileges commensurate with the level of access requested. When a person attempts to access protected information, their access rights are compared with the access rights required by that information. The access control capability then must determine if permissions/access attributes that the person possesses are equal to or dominate those required for access to the specific protected areas, assets, or system-related items within the controlled system.

Accountability Management

Access Management includes management of the access control audit trail. Accountability management involves determining which security relevant events a required for collection, which events are optional, the frequency of reporting to the access control audit collection sub-capability, the management of user audit profiles, the configuration of review frequency, alarms, statistical reporting, the establishment of specific rules for enhanced audit (e.g. upon identification of a perceived threat or attack profile, upon declaration of an *emergency access* situation, or as needed to configure monitoring of specific activities such as for fraud detection).

Provisioning

Access management includes identity provisioning. Provisioning refers to the process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the creation, modification, deletion, suspension, and restoration of a defined set of accounts or attributes. Provisioning of user access control credentials refers to the creation, maintenance, correlation, synchronization and deactivation of user-objects and user-attributes, as they exist in one or more systems, directories or applications, in response to an automated or interactive business processes. Provisioning software may include one or more of the following processes: change propagation, self-service workflow, consolidated user administration, delegated user administration, and federated change control. Provisioning is typically a subsystem or function of an identity management system that is particularly useful within organizations where users may be represented by multiple user objects on multiple systems.

Secure Identity Management

Access management includes the capability to uniquely identify an individual and restrict his or her access to resources in the iEHR system based on his or her established identity. The functions of Identity management include identifying individuals as users in the EHR IT system, controlling access to the resources in that system, authenticating users and granting or denying access permissions based upon user role-profile attributions and access authorization levels. This capability provides for the safeguarding and managing of individuals' personal and health information. The capability includes:

- Clinical Patient Identity Management (PIN) which is a set of business processes and a supporting infrastructure to create, maintain, and use digital identities, uniquely identify patients, and resolve prevent identity problems via matching
- Person identity management, which is a set of business processes and a supporting infrastructure to create, maintain, and use digital identities and uniquely identify persons other than patients (doctors, nurses, employees, etc.) to prevent identity problems
- Role/attribute-based identity management: A set of business processes and supporting infrastructure to properly identify clinical organizations, departments, patients, health employees, and care providers to authorize access to health information systems and networks. This type of access management provides the ability to share subsets of this information with certain customers, vendors, and partners as needed, so the information available can be adapted to the particular user or group
- Data segmentation/attribute management: A set of business processes and supporting infrastructure to properly manage metadata tagging of health information systems that provides the ability to share subsets of this information with certain customers, vendors, and partners as needed, based upon managed Federal, organizational, business and patient rules.

3.2 Identity Management

The DoD/VA Patient Identity Management service will provide consistent methods for identifying persons and maintaining the associated identity attributes for these individuals across the two organizations, to support the delivery of healthcare and benefits. Patient safety principles introduce iEHR specific requirements for identity management.

PIM is a fundamental enabling capability for the delivery of all iEHR capabilities. DoD and VA will develop a unified suite of PIM services based upon joint agency requirements and business rules. Services provided will allow iEHR consuming applications to consistently search for a person known to DoD/VA, add a person if unknown, and update identity traits where appropriate. In addition, services will be provided to maintain identifiers and the correlation of person identity records across both agencies, to support access to agency systems, the Nationwide Health Information Network (NwHIN) and other Federal systems as needed. PIM will also provide automated tools for the resolution of identity issues, such as overlaps and overwrites, and maintain the accuracy of a joint agency person view.

PIM provides the ability to uniquely identify and enumerate an individual for Identity purposes, and to maintain the integrity of their identity (identifiers and traits) and the integrity of their records across iEHR for both agencies. As such, this capability provides for the management of individuals' personal identifiers, identity information and their subsequent health information and includes:

- A set of business processes and a supporting infrastructure to create, maintain, and use digital identities, uniquely identify patients, and identify and resolve identity problems (overlap, overwrite, etc.)
- A set of identity management functions including the identification of individuals in a system, the management of the quality of the traits that identify the individual, the management of the resolution of duplicate identities and other identity issues, and management of the relationships between identities, either internal to DoD/VA or external to DoD/VA

3.3 Network and Security

The network security architecture capability encompasses the planning and design of the organization's network to reduce security risks in accordance with the organization's risk analysis and security policies. It describes the network segmentation (i.e., security zones) and security layers (i.e., access control, intrusion prevention, content inspection, etc.). It details which security services are needed in a particular system.

Network and security architecture includes authorization, access, and identity management requirements and functions for the system, and how and where these requirements are implemented. This is based on expected risks or scenarios and how and where those risks or scenarios may be encountered. The capability establishes security standards that can be leveraged in a useful fashion over a long period of time.

The system's security architecture should be adaptable and should take into consideration the trade-offs between achieving system goals and mitigating risk. It focuses on reducing security risks and enforcing policy through the construction of firewalls, routers and other network equipment. This capability provides the means to enforce all DoD and VA's security policies and procedures in order to protect their information.

3.4 Single Sign On/Context Management (SSO/CM)

It is the intent of the iEHR to leverage SSO/CM for all applications that do not possess SSO/CM functionality natively.

The SSO/CM capability enables a user to access multiple applications after signing in only once, for the first time. SSO is directly related to access and control and identity management because when a user goes through the act of signing on, their identity is recognized, and they no longer need to sign in again to gain access to any of the connected systems.

Information from different applications within the iEHR is synchronized and is available together for a user to see. The user will need to provide a User-Identification (ID)/password combination, a Personal Identification Verification (PIV) card, or a Common Access Card (CAC) for access to the system. Once a user has entered their credentials and the credentials have been verified, the user will not need to provide the credential again to open any of the clinical applications. Once users log out of the single sign-on application, all other open clinical applications will shut down gracefully.

The context management capability allows clinicians to choose a patient once in one application and have all other applications containing information on that same patient activate the data they contain. Context management obviates the need to redundantly select the patient in the varying applications. When a clinician opens multiple applications, the applications open with the patient context of the first application that was open. The application prompts screen savers and logouts over a period of user inactivity.

3.5 Virtualization

The MHS Enterprise Virtualization initiative is designed to provide a uniform and universal platform on which MHS applications will be delivered. The platform virtualizes both applications and servers, enabling health care providers and other authorized users to obtain secure and stable user access to Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), Third Party Outpatient Collection System (TPOCS), Coding Compliance Editor (CCE), Nutrition Management Information System (NMIS), Special Needs Program Management Information System (SNPMIS) and various other clinical applications. MCiS will host the MHS virtualization platform at 20 geographical MHS Application Access Gateway (MAAG) sites worldwide in order to regionalize and consolidate MHS applications and servers into a unified, robust, and scalable computing infrastructure. The MAAG architecture will provide a more efficient, effective and secure delivery of MHS applications while also improving the availability and maintenance of a complete and accurate health record for the MHS beneficiary population.

The virtualization effort is based on a common computing and storage infrastructure that enables standardized access to current MHS applications and the flexibility to access those applications from anywhere. Virtualization will promote centralized management and monitoring of the MHS application delivery, which results in standardization and decreased desktop support activities across the enterprise, as well as a decreased time to market for future applications.

3.6 Common Information Interoperability Framework (CIIF)

The CIIF of the iEHR is intended to enable the reliable, context-sensitive management and delivery of semantically-interoperable clinical information and terminology; this is suitable for 75 years or more of an individual’s healthcare VLER, Clinical Decision Support (CDS) for patient care, clinical research, and epidemiological studies, where patient data must be clear, complete, concise, correct and consistent. CIIF has two core components: a system of standards-based clinical terminology and detailed clinical information models. The clinical terminology is based primarily on Systematic Nomenclature of Medicine (SNOMED) and other federally designated standards (e.g., LOINC, RxNorm); while the detailed clinical information models are designed to sensibly describe clinical findings and events with appropriate terminology bindings and context metadata. CIIF uses the combination of the information model and terminology components to provide healthcare providers with global, seamless, information sharing in a manner that can significantly improve the quality of care provided. The following artifacts speak to common data standards, common information models, common terminology models, information exchange specifications, translation services, and VLER requirements/sharing data.

3.7 Health Data Dictionary (HDD) and Custodial Agent (CA)

In an effort to establish computable data, permit accurate, compliant, and efficient business intelligence, clinical decision support, Force Health Protection (FHP) and researchable population health data, the IPO has made the 3M HDD software and Core HDD Content a publicly accessible resource and 3M the initial HDD (CA) for the HDD Software and Core HDD Content. The 3M HDD will provide the joint enterprise a practical, scalable and operational semantic interoperability solution for DoD/VA iEHR, VLER, and for communication with commercial solutions using supported protocols and interfaces. 3M, as the HDD CA, will prepare, facilitate and manage the use of the Open Source HDD Software and its publicly accessible Core HDD Content.

3.8 Virtual Lifetime Electronic Record (VLER)

VLER Health Strategy

The VLER vision is seamless sharing for of an individual's comprehensive, standards-based interoperable health information for health care providers in DoD and VA.

- Short term: Develop and deploy technical and business improvements for Legacy EHR platforms for health data interoperability for:
  - NwHIN Exchange
  - NwHIN Direct
- Long term: Develop and implement technical applications and business processes for health information exchange from the iEHR platform

<u>Various VLER extracts/program descriptions:</u>

VLER will create a secure exchange for electronically sharing and proactively identifying health and benefits entitlements for service members, Veterans, and their eligible dependents, from accession through final honors. Ultimately, VLER will allow Veterans, their dependents, beneficiaries, care givers, clinicians, and benefit providers to view all relevant information about the Veteran seamlessly, regardless of where it was documented, in a single, secure, electronic record.

VLER Major Initiative Site:

http://vaww.oed.portal.va.gov/products/vler/Pages/welcome.aspx

VLER Health is a program that shares certain parts of your health record between the Department of Veterans Affairs (VA), Department of Defense (DoD) and selected private health care providers over a secure network known as the Nationwide Health Information Network.

VHA VLER Health Brochure:

http://vaww.vhaco.va.gov/oia/docs/HI/CHIO_VLER_Health.pdf

The VLER initiative will offer a new way for health care providers to collaborate with one another as they provide care for our service members and Veterans. It will promote the efficient exchange of information, reducing the burdens placed on service members and Veterans while improving the continuity of care they receive.

VLER is not a single system, but an initiative to share health care data by use of common standards. VLER will ultimately enable authorized users within DoD, VA, private health care providers, and other government agencies to share health, personnel, and benefits information. The initiative will also improve the delivery of health care and benefits to service members and Veterans, as well as their eligible designees.

DoD VLER FAQ:

http://www.prim.osd.mil/Documents/VLER_FAQs.pdf

The VLER initiative is a capability that allows service members' and Veterans' electronic health and administrative (personnel and benefits) information to be shared seamlessly among the Department of Defense (DoD), Department of Veterans Affairs (VA), and other federal and private providers.

VLER Health will:

- Allow multidirectional exchange of health and benefits information among private health care and benefits providers, VA Medical Centers and administrative offices, and DoD Medical Treatment Facilities, improving the continuity of care and benefits adjudication
- Offer a more complete picture of a Service Member's or Veteran's medical history and benefit eligibility regardless of where he or she received health care or benefits guidance
- Take the burden off the service member or Veteran for carrying paper copies of records from one office to another
- Provide a common access point for a patient's electronic health information and proactively recommend certain benefits to which a service member or Veteran could be eligible

VLER is not a new records management system, or even a new set of records. Instead, VLER allows existing systems owned by different organizations to communicate with one another.

DoD VLER Trifold Brochure:

http://www.prim.osd.mil/Documents/VLER_Trifold_Brochure.pdf

Link to ONC Direct Project:

http://wiki.directproject.org/ONC+Website

3.9 SOA/SOE/Enterprise Service Bus (ESB)

The solution shall conform to applicable DoD, VA, and iEHR goals, standards, constraints, and other requirements and align with guidance and processes provided in the following attachments:

- SOA Suite ESB-Protocols and Standards–This is a list of standards and protocols supported by the SOA Suite/ESB solution with which future solutions must integrate
- SOA Suite-Adaptor Support for External Systems–This list of adaptors that are inherently supported by the SOA Suite/ESB solution set is not a set of requirements, but rather an informational list to assist in assessing the level of effort required to integrate external products into the iEHR SOA

- MHS SOE Reference Architecture –This reference architecture document provides an alignment target for MHS implementations and serves as a draft starting point for the iEHR reference architecture
- iEHR SOA Suite Implementation View–This artifact complements the reference architecture by providing an implementation view for the proposed SOA suite solution and serves as an alignment requirement for future solutions
- Registry Service Description Document–This service description document is a proposed requirement (proposed by the SOA work stream in the architecture and engineering IPT under the IPO) and serves as guidance based on being a draft requirement for a future solution's alignment
- iEHR Service Oriented Infrastructure (SOI) Governance–This SOI governance document is proposed guidance with embedded requirements, is proposed by the SOA work stream of the architecture and engineering IPT, and serves as guidance based on being a draft requirement for a future solution's alignment
- iEHR Candidate SOA Software Services–This list of candidate services is subject to change, and provides guidance on possible services with which future solutions must integrate and serves as guidance for the future solutions

The contractor shall adhere to goals, standards, constraints, guidelines, policies, architectural products, and processes established and approved for the iEHR, provided to the contractor as Government Furnished Information (GFI) when available.

3.10 Portal Framework

The portal framework refers to the infrastructure components (hardware, software, networks, tools, toolkits, processes, and documentation) needed to implement, operate, manage, and sustain iEHR presentation layer capabilities. Conceptually, the iEHR Portal is the gateway or entry point into iEHR business capabilities and longitudinal patient record applications and information for providers, patients, and other stakeholders/users. The iEHR portal framework infrastructure will enable implementation of the iEHR presentation layer (graphical user interface), and will provide enabling portal and web technologies to support this presentation layer.

The Portal will provide a uniform and integrated entry point to *Content* (e.g. health resources, data, services, and applications). Within the healthcare domain, it will provide an entry or access point for patients, providers, administrators, business partners, trusted agents, the general public, or other user types to access information and conduct business from a single, logical entry point.

Enterprise portals typically deliver a number of enabling capabilities or services including:

- Personalization–User tailored presentation services and customization
- Content and application aggregation and integration–Consolidation and integration of applications and data from disparate sources into one or more pages
- Web application development platform unification–A standards-based environment for developing web, portlet-based, and mobile web applications and presentation layers
- Web portal consolidation framework–A platform and infrastructure for consolidating portals

3.11 Presentation Layer

It is the intent of the iEHR to utilize the portal framework for delivery of all applications and services through a common presentation layer. The presentation layer capability provides a single point of computer entry that will interface with all desired iEHR capabilities for the end users. Information from different applications within the iEHR is synchronized and will be available together as a single record.

The GUI capability provides an interface so that users can access automated tools used for results interpretations from lab, radiology, or other medical diagnostic tests.

A key feature of a presentation layer is its ability to support the delivery of care by enabling prior information to be found and displayed meaningfully. iEHR systems should facilitate search, filtering, summarization, and presentation of available data needed for patient care. Systems should enable views to be customized; for example, specific data may be organized chronologically, by clinical category, or by consultant, depending on need. Jurisdictional laws and organizational policies that prohibit certain users from accessing certain patient information must be supported.

Users can also tailor the way they view information and set default views based on their function and the type of information they typically require. This function takes into account laws and policies that restrict which users have access to certain data. Users have tools to locate specific information, such as mechanisms for searching, filtering, summarizing, and presenting data. The arrangement of data can be customized for specific situations, such as by date, provider, or service. Finally, the system allows users to select which data from the health record should be included in reports, either in hardcopy or in electronic output.

- All capability developments will be delivered in the form of portlets and optionally in web applications to have a presence on iEHR presentation layer. Web applications not delivering associated portlets will have only a hyperlink on the presentation layer.
- iEHR will provide Portlets Software Development Toolkit (SDK) and a guideline for Look-Feel-Behavior (RFB) Standards. The SDK will be based on a portal product selected for IOC. RFB standards will be developed by presentation layer C-IPT in coordination with a PL engineering support team.
- iEHR will provide SOA governance and SOA Catalog of existing services that developers shall consume in developing portlets (for cost reduction and agile development). Developers shall have the ability to produce SOA services for other developers to consume (for future cost reduction and agile development) and will be incentivized for the production.
- The presentation layer does not include the development of clinical or non-clinical capabilities but includes the integration of portlets compliant with iEHR guidelines and the assurance of operable SSO/CM, user authentication, and access management within the presentation layer portal framework.

3.12 Data Infrastructure

On February 26, 2010, the Office of Management and Budget (OMB) announced the Federal Data Center Consolidation Initiative (FDCCI) with the goal of reducing the number of federal data centers 40 percent by 2015. To comply with this Federal mandate, the iEHR data infrastructure will build upon plans already underway at MHS and VA focusing on data center consolidation – with a goal to reduce the overall data center count by 90 percent.

To accomplish this, the iEHR infrastructure will rely on a blend of data center co-location and server consolidation. The key factors of the iEHR infrastructure will revolve around the following items.

- Use of public cloud infrastructure (e.g., Amazon EC2, ATT)
- Use of private cloud infrastructure (e.g., DISA RACE)

- Use of traditional data center infrastructure (e.g., MHS Military Treatment Facility (MTF) data centers)

The future state architecture is not intended to be a pure version of any of the previous options, but rather a hybrid solution optimized to address the lifetime program costs (e.g., utility pricing of elastic cloud service, data center operation and maintenance costs) and capability-specific benefits (e.g., order entry transactional processing advantages, latency of medical imaging activities). As such, the specific blend of these components in the final iEHR data infrastructure will be derived from a cost-benefit evaluation conducted in the future as well as requirements developed by the functional teams.

3.13 Development Testing Center (DTC)/Development and Test Environment (DTE)

Vendor developed software will be constructed to properly function in both federated and regionalized versions. All software testing in the environments outlined below will consider testing complete when developed requirements pass on both a federated or base platform and in a *regionalized* setting that may include a local MTF network or interface considerations. The vendor will need to build and or support product testing in the following environments:

Development – Stage 1

This is the vendor environment that contains their client developed requirements or code. As code is developed and validated a CM tool will be utilized to store or check-in functioning code as it becomes available. This environment is the initial development ground for base code.

Development Integration Test (DIT)–Stage 2

The developed client requirements or code that has been validated by the Lead Developer will be promoted to the DIT environment. The vendor will be responsible for confirming which client applications will be tested in conjunction with the requested developed requirements for interface, pass-thru or workflow testing as well as validation for the newly developed coded if it is new functionality, an enhancement or repair for a stand-alone software application. All developed and/or altered software code must be tested by development for functional and technical integrity in DIT prior to release to the Test and SIT environments. This environment will replicate or mirror the production environment. This is the second core environment migration in the development life cycle.

Test – Stage 3

This environment will support functional and technical requirement validation of the developed code in an environment that is separate from all development environments. Typically, the test environment is utilized by the testers for functional and technical requirements validation prior to a larger integrated product or systems test. This environment sometimes contains other applications and will be identical to the production environment. The Test Environment can sometimes be used in lieu of the SIT environment described below. Depending on the software code being developed (stand-alone or integrated with other components or interfaces), developed code can be tested in the test environment by the test team for initial validation. Once validated (and when interface or component testing is needed) the code can be migrated to the Software Integration Test (SIT) environment for more focused and/or rigorous process/interface test validation.

Software Integration Test (SIT) – Stage 4

A separate testing environment utilized by the testers to validate new software functionality, code repairs and/or enhancements. This environment will replicate or mirror the production environment. SIT validation typically includes all functional and technical testing of developed requirements with dependent and independent software applications and/or interfaces to ensure that the new or enhanced code will seamlessly function and pass data to other DoD and/or VA applications/systems. The SIT environment is typically the last validation ground prior to releasing the developed software into production. Some code changes may require a limited user test in SIT and/or the production environment with the vendor/development team providing support as needed.

Training and Demonstration – The *Sandbox*

This environment may include just a subject application or a system suite that is representative of the production environment. Its purpose is to provide the user's a realistic training ground to learn basic application/system functionality and/or to learn how changed/enhanced code now performs as a developed new requirement. Test data in this environment is either masked production data stripped of key PII or generated/dummy test data with data triggers for each application under test.

This environment is also beneficial for demonstrating to stakeholders how the code will function in production. The vendor will also be responsible for following standard CMMI processes for versioning and storage of working or developed code.

4.0 Clinical Requirements

4.1 Laboratory Capability

Laboratory

The laboratory capability includes the principal medical diagnostic laboratory testing and transfusion functions, and sets the standards for quality, test methods and procedures for laboratory testing for patient care in the medical center and supported clinics. The laboratory must analyze physical specimens in order to facilitate diagnosis, treatment, and recovery from disease, as well as to maintain health. Laboratories may exist within hospitals or clinics, or may exist as separate facilities. Specimens are obtained from individuals and may include blood, urine, and tissues. These specimens are analyzed for the presence or absence of certain elements or for critical levels of elements or anomalies.

The laboratory capability is used to request tests for patients, keep track of patient or specimen histories, and print test results for patients and providers. Records must be kept of every laboratory test and should include patient information, potential diagnosis, the tests performed, type of specimen collected, time the specimen was collected, and any specific instructions or precautions. The entire laboratory history must be viewable in a patient's medical record. Patients are identified at the time of arrival and the specimens are identified by a numbering system that links specific specimens with the related patient. Specimens taken at bedside in a hospital and sent to the laboratory also require proper identification within the capability.

The laboratory capability must allow for interoperability across all departments and sections of both anatomic and clinical pathology such as autopsy pathology, surgical pathology, cytopathology, clinical chemistry and special chemistry, hematology, immunology, microbiology, and transfusion medicine. There are also specialized laboratories that are devoted to molecular diagnostics (viral load testing), toxicology, flow cytometry, and electron microscopy.

Anatomic Pathology

The anatomic pathology capability includes the ability to analyze and process information on the diagnosis of diseases based on the examination of tissues and organs. It is a medical specialty that is concerned with the diagnosis of disease based on the gross, microscopic, chemical, immunologic, and molecular examination of organs, tissues, and whole bodies. Pathology and laboratory medicine services provide the principle medical diagnostic laboratory testing and transfusion functions, and set the standards for quality, test methods, and procedures for laboratory testing for patient care in the medical center and supported clinics, which may include deployed labs.

The anatomic pathology capability shall interact with a blood bank system or other source to support orders for blood products or other biologics including discontinuance orders. Blood bank or other functionality that may come under jurisdictional law or other regulation (e.g. by the Food and Drug Administration (FDA) in the US) is not required. Functional communication with such a system is required.

An additional function of the anatomic pathology capability is support for accurate specimen collection, which ensures the accuracy of specimen collection, and positive identification of the patient and specimen. The provider is notified in real-time of potential collection errors such as wrong patient, wrong specimen type, wrong means of collection, wrong site, and wrong date and time.

Information related to the iEHR joint requirements for the Lab capability is included within the architecture standards compliance framework, and should be reviewed by the vendor in order to understand the following:

- Joint lab requirements
- Interfaces and protocols used for legacy lab capability
- Technical standards and service levels for supporting common infrastructure

4.2 Pharmacy Capability

Information related to the iEHR joint requirements for the pharmacy capability is included within the architecture standards compliance framework, and should be reviewed by the vendor in order to understand the following:

- Joint lab requirements
- Interfaces and protocols used for legacy lab capability
- Technical standards and service levels for supporting common infrastructure

4.3 Immunization Capability

Immunization

The immunization capability includes the ability to identify, administer, document, and monitor the appropriate immunizations and adverse events based on a beneficiary's stage of life or travel-related deployments. Each immunization is prescribed and administered by licensed medical personnel and accurate records are kept all immunizations administered. Records include information such as injection site, vital signs, pain assessments, and immunization product information. Any observations or details of medical decision-making are also recorded.

Immunizations may be administered through several different types of patient encounters, including an emergency department visit, a well-child exam, a pre-deployment readiness appointment, inpatient care, or a routine primary care visit. All immunizations administered will be tracked and monitored. The system will assist in the management of immunization administration and make immunization information available to healthcare providers. Additionally, the electronic medical record will provide the ability to assist the provider in decision support so that the correct immunization is given at the right time.

Additional functions of the Immunization capability include:

- <u>Create and maintain patient-specific immunization lists</u>: Immunization lists shall be managed over a period of time, including over the course of a visit or stay, and maintained for the lifetime of the patient. Details of immunizations administered shall be captured as discrete data elements and the entire immunization history shall be viewable
- <u>Manage immunization administration</u>: The system shall capture and maintain discrete data concerning immunizations given to a patient including date administered, type, manufacturer, lot number, and any adverse reactions. It shall facilitate the interaction with an immunization registry to allow maintenance of a patient's immunization history
- <u>Provide support for medication and immunization administration</u>: The capability shall alert providers to potential administration errors (such as wrong patient, wrong drug, wrong dose, wrong route, and wrong time) in support of safe and accurate medication administration and the surrounding workflow. Information related to the iEHR joint requirements for the Immunization capability is

included within the architecture standards compliance framework, and should be reviewed by the vendor in order to understand the following:

- Joint Immunization requirements
- Interfaces and protocols used for legacy Immunization capability
- Technical standards and service levels for supporting common infrastructure

4.4 iEHR Certification/Meaningful Use

The iEHR system shall be certified and be compliant with the standards and certification criteria issued by the US Department of Health and Human Services (DHHS), and shall maintain that certification throughout its lifecycle. iEHR certification includes meaningful use requirements.

The system shall adhere to all meaningful use objectives and standards for eligible providers and eligible hospitals (42 Code of Federal Regulations (CFR) 495.6(d)-(g)) as published or modified through the Office of National Coordinator (ONC) from the Health Information Technology (HIT) Policy (HITPC) and HIT Standards (HITSC) Committees, as well as certification criteria (45 CFR 170.302, 170.304, and and170.306) and standards (45 CFR 170.205, 170.207, and 170.210).

4.5 Healthcare End-User Usability

The driving purpose in the creation of the iEHR is to be usable by the healthcare end-user and facilitate patient-centered healthcare. The International Organization for Standardization (IOS) defines usability as ‘‘the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use,’’ (IOS 9241–11).

Usability as applied to iEHR is defined in the following requirements:

Optimize clinical workflow:

- Decreasing the duration of the workflow process
- Ability to enter both structured and unstructured data via authoritative routes including self-entered patient data and approved mobile devices
- Ability to efficiently create and modify clinical templates
- Ability to enter data via customized clinical templates
- Decreasing the steps required to complete the clinical workflow process either for an individual patient encounter or work load of a clinical practice
- Improving patient clinical outcomes
- Data elements should only be entered once and avoid entering the same information multiple times
- Availability of iEHR at all times, including the ability of the healthcare team, caregiver, service member/veteran to communicate effectively in between care encounters

Optimize clinical practice analysis:

- Capturing of structured data enables easy customization and generation of ad hoc or template reports that provide feedback on any metrics designated utilizing standardized data elements and filters to multiple levels of summarization defined at the facility (e.g., provision of medication management plans to patient, individual provider’s practice, team’s practice, clinic, facility, multiple sites, etc.)
- Ability of end-user to efficiently and easily produce reports
- Ability to export reports or data and be able to manipulate with analytical and other applications. In order to achieve the usability requirements described above, the design and development of the system shall include a User-Centered Design (UCD) process based on human factors. The proposed

rule for meaningful use stage 2 requires iEHR technology developers to select and employ a UCD process as defined in documents and requirements such as IOS 9241-111, ISO 13407, IOS 16982, and NIST 7741

- The common characteristic of a UCD includes activities aimed at understanding the user, the user's tasks, and the user's environment; iterative design and formative usability testing; user risk analysis; and a summative validation usability testing

As part of the UCD activities for iEHR, the business owners specifically identified the following:

- Conduct a like-system review of cardiovascular assessment, reporting and tracking system for Cath Labs (CART-CL) (used in VA cardiac labs and also deployed at Nellis Air Force Base (AFB) to inform the design of the iEHR system
- The system shall undergo summative validation testing activities that include usability testing with end users in the actual environment. (As a reference, see the functional certification program by clinical informatics and requirements division of the interagency program office and the integrated clinical informatics board)

4.6 Patient Driven Care and Care Coordination

The system shall have the capability of incorporating patient self-entered data where relevant, in order to provide context-specific care. This may include results of home monitoring and patient-reported functional outcomes (e.g., VR-12, FIM, PHQ-9, Patient Reported Outcomes Measurement Information System (PROMIS), etc.) in a structured format. The system shall support adoption of authoritative source of patient self-entered data so that end users may seamlessly traverse the system's many applications. The system must capture in standard format (e.g., HL7 Clinical Document Architecture (CDA) the plan of care which will be shared with the patient and members of the treatment team (e.g., treatment goals such as target blood pressure, cholesterol, blood glucose, etc.; medication use, including medications prescribed outside of the iEHR setting; barriers to medication adherence; history of adverse drug events, reactions, and allergies). The system shall have the capability to generate, at all levels, a list and summary of all patients meeting defined criteria (e.g., diagnosis of diabetes), for purposes of panel management and care coordination. The system shall be compliant with and support the criteria of the National Committee for Quality Assurance (NCQA) for Patient Centered Medical Home (PCMH), Level 3 recognition program.

4.7 Cognitive Support/Knowledge Management/Clinical Decision Support

The system shall provide ready access to cognitive support and knowledge tools including VA-DoD evidence-based practice guidelines, alerts and reminders, treatment algorithms, clinical protocol/pathway support, drug and disease reference information and guidance, documentation forms/templates and order/prescription creation facilitators, patient risk calculators, and other expert systems that may be developed over time. CDS tools should be guidance-oriented, context-sensitive, and designed with workflow, patient safety, and patient-centered care in mind. CDS tools will be utilized in a manner consistent with usability criteria in section 8.3.9, and provide CDS at key points within the clinical workflow without causing hindrance.

Cognitive support for health care professionals and patients will be model driven and will help end users place the data into context in ways that make clinical sense for that patient and support shared decision-making between patient and clinician. CDS tools will build upon model driven cognitive support to integrate patient-specific data and evidence-based practice guidelines and research results into daily practice. The system shall provide relevant information to prevent frequent, defined clinical errors and function to address patient safety, improved quality, improved efficiencies and cost reductions. It shall facilitate the users' ability to do what is *right* and make it difficult to make errors in the provision of best practice healthcare. To that end, the system shall rely on guidance-based methods and provide recommendations based on Clinical Practice Guidelines (CPGs)/diagnosis/standard treatment options, but avoid interfering with patient treatment decisions. The guidance shall be tailored to be as specific as possible to the patient being treated utilizing patient specific data-relevant labs, the problem list, relevant medications, antimicrobial profiles, and context-specific diagnostic and treatment recommendations.

CDS may be one of two main types: specific alert guidance and current knowledge based (i.e. diagnosis or treatment utilizing specific patient data). They utilize CPGs and recognized treatment protocols in guiding the end-user to present available order sets and utilize alerts only when deviating from those protocols or when the options are selected outside of the guidance. The system shall capture and track this data with the additional ability to change the CDS within the iEHR as necessary to conform to recent clinical research. The CDS should be centralized so that modifications only have to be entered once rather than changed in each capability. It is important that there is flexibility in the CDS capability in order to stimulate innovation and include emerging capabilities (e.g., predictive modeling, text mining, population and public health, mobile tools for remote activity monitoring) and data integration.

4.8 Business Intelligence/Analytics

The iEHR system requires the capability to generate the Clinical Quality Measures (CQMs) specified by meaningful use as well as other aggregate reports needed for quality monitoring and performance accountability. Structured clinical data will be collected according to recognized standards within meaningful use (e.g., SNOMED, LOINC, RxNorm, etc). The iEHR system requires population-based reporting tools that are relevant, adaptable and easily used by the end-user.   The iEHR system requires the capability to identify, track, and report aggregate performance stratified by key patient characteristics such as gender, race/ethnicity, benefit category, diagnostic categories (e.g., mental illness diagnoses, etc.) and other factors, in order to track health disparities and address the needs of vulnerable populations. It is imperative that impact on workflow is tracked when modifications are made to the iEHR system.

5.0 Privacy, Security & Information Assurance Requirements

5.1 Privacy and Security

The system shall meet the privacy and security standards within meaningful use and comply with the requirements of the NwHIN.

Special requirements for protected health information (DoD only):

- A Data Sharing Agreement (DSA) is currently used to request and control the disclosure, use, storage and/or destruction of MHS data that is owned and/or managed by Tricare Management Activity (TMA) to ensure that applicable privacy and security requirements are followed. In addition, research requests for MHS data that include protected health information (PHI) must be reviewed for HIPAA compliance by the TMA Privacy Board.
- Under DoD 6025.18-R, *DoD Health Information Privacy Program*, January 24, 2003, reasonable steps must be taken to implement appropriate procedural, administrative, technical and physical safeguards to prevent the unauthorized use and/or disclosure of any personally identifiable information (PII) or PHI. Likewise, all uses, disclosures, and destruction of PII and PHI data are generally subject to DoD 5400.11-R, *DoD Privacy Program*, May 14, 2007, as well as DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003, and DoD 8580.02-R, *DoD Health Information Security Regulation*, July 12, 2007.
- To begin the DSA request process, the contractor should choose the applicable request template at http://www.tricare.mil/tma/privacy/Templates.aspx, or should contact duamail@tma.osd.mil. After receiving DSA approval, anyone needing access to information system applications or data sources must contact the responsible system program office. DSAs are active for one year, or until the end of the current option year, whichever comes first. If the DSA will not be renewed, the TMA contractor must provide a Certificate of Data Destruction (CDD) to the TMA privacy and civil liberties office (Privacy office).

Business Associates (DoD Only)

The TMA Privacy Office website at http://www.tricare.mil/tma/privacy/downloads/BusinessAssociateAgreement.doc contains the following standard contract language regarding business associates.

Introduction

In accordance with DoD 6025.18-R *DoD Health Information Privacy Regulation*, January 24, 2003, the contractor meets the definition of business associate. Therefore, a Business Associate Agreement (BAA) is required to comply with both the HIPAA privacy and security regulations. This BAA serves as that agreement whereby the contractor agrees to abide by all applicable HIPAA privacy and security requirements regarding health information as defined in this BAA, and in DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

Definitions: As used in this BAA, generally refer to the CFR definition unless a more specific provision exists in DoD 6025.18-R or DoD 8580.02-R.

Individual has the same meaning as the term *individual* in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information (SPIIHI) at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information (PHI) has the same meaning as the term *protected health information* in 45 CFR 160.103, limited to the information created or received by the contractor from or on behalf of the Government pursuant to the contract.

Electronic PHI has the same meaning as the term *electronic protected health information* in 45 CFR 160.103.

Required by Law has the same meaning as the term *required by law* in 45 CFR 164.103.

Secretary means the Secretary of the Department of HHS or his/her designee.

Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160 and part 164, subpart C.

Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in 45 CFR 160.103, 160.502, 164.103, 164.304, and 164.501.

- The contractor shall not use or further disclose PHI other than as permitted or required by the contract or as required by law.
- The contractor shall use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this contract.
- The contractor agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits in the execution of this contract.
- The contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the contractor of a use or disclosure of PHI by the contractor in violation of the requirements of this BAA. These mitigation actions will include as a minimum those listed in the TMA breach notification Standard Operating Procedure (SOP), which is available at: http://www.tricare.mil/tma/privacy/breach.cfm
- The contractor shall report to the Government any security incident involving PHI of which it becomes aware.
- The contractor shall report to the Government any use or disclosure of the PHI not provided for by this contract of which the contractor becomes aware.
- The contractor shall ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the contractor, on behalf of the Government, agrees to the same restrictions and conditions that apply through this contract to the contractor with respect to such information.
- The contractor shall ensure that any agent, including a subcontractor, to whom it provides electronic PHI, agrees to implement reasonable and appropriate safeguards to protect it.
- The contractor shall provide access, at the request of the Government, and in the time and manner reasonably designated by the Government to PHI in a designated record set, to the Government or, as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524.

- The contractor shall make any amendment(s) to PHI in a designated record set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government, and in the time and manner reasonably designated by the Government.
- The contractor shall make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the contractor, on behalf of the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner reasonably designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the privacy rule.
- The contractor shall document such disclosures of PHI and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.
- The contractor shall provide to the Government or an Individual, in time and manner reasonably designated by the Government, information collected in accordance with this BAA, to permit the Government to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

<u>General Use and Disclosure Provisions</u>

Except as otherwise limited in this BAA, the contractor may use or disclose PHI on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of PHI would not violate the HIPAA Privacy Rule, the HIPAA Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government.

<u>Specific Use and Disclosure Provisions</u>

Except as otherwise limited in this BAA, the Contractor may use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

Except as otherwise limited in this BAA, the Contractor may disclose PHI for the proper management and administration of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

The Government shall not request the Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule, the HIPAA Security Rule, or any applicable Government regulations (including without limitation, DoD 6025.18-R and DoD 8580.02-R) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this BAA.

Except as otherwise limited in this BAA, the contractor may use PHI to provide data aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

Business associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Obligations of the Government

<u>Provisions for the Government to Inform the contractor of privacy practices and restrictions</u>:

- The Government shall provide the contractor with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520.
- The Government shall provide the contractor with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect the business associate's permitted or required uses and disclosures.
- The Government shall notify the contractor of any restriction to the use or disclosure of PHI that the Government has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by the Government:

The Government shall not request the contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule, the HIPAA Security Rule, or any applicable Government regulations (including without limitation, DoD 6025.18-R and DoD 8580.02-R) if done by the Government, except for providing data aggregation services to the Government and for management and administrative activities of the business associate as otherwise permitted by this BAA.

Termination:

A breach by the contractor of this BAA, may serve as basis for termination of this agreement.

Effect of Termination:

- If the BAA has records management requirements, the records subject to the BAA should be handled in accordance with the records management requirements. If the BAA does not have records management requirements, the records should be handled in accordance with the following two bulleted paragraphs.
- If the BAA does not have records management requirements, except as provided in bullet (3) of this section, upon termination of the BAA, for any reason, the business associate shall return or destroy all PHI received from the Government, or created or received by the business associate on behalf of the Government. This provision shall apply to PHI that is in the possession of second tier business associates or agents of the business associate. The business associate shall retain no copies of the PHI.
- If the BAA does not have records management provisions and the business associate determines that returning or destroying the PHI is infeasible, the business associate shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the business associate that return or destruction of PHI is infeasible, the business associate shall extend the protections of the BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the business associate maintains such PHI.

Miscellaneous:

Regulatory References: A reference in this BAA to a section in DoD 6025.18-R, DoD 8580.02-R, privacy rule or security rule means the section currently in effect or as amended, and for which compliance is required.

Survival: The respective rights and obligations of business associate under the *Effect of Termination* provision of this BAA shall survive the termination of the agreement.

Interpretation: Any ambiguity in this BAA shall be resolved in favor of a meaning that permits the Government to comply with DoD 6025.18-R, DoD 8580.02-R, the HIPAA privacy rule or the HIPAA Security Rule.

External References:

(NISTIR 7741) NIST Guide to the Processes Approach for Improving the Usability of Electronic Health Records

Search Portal

http://www.nist.gov/publication-portal.cfm

NISTIR 7741 Document

http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907313

Patient Health Questionnaire PHQ-9: Search portal

http://www.integration.samhsa.gov/search?query=phq-9

PHQ-9 Document

www.integration.samhsa.gov/images/res/**PHQ**%20-%20Questions.pdf

International Standard ISO 9241-11

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=53372

HL7 CDA (Search File Name HIMSS2010)

http://www.hl7.org/search/index.cfm?searchFacets=FileType_pdf&criteria=HIMSS2010

5.2 Software Assurance/Information Assurance

5.2.1 Software Security, Certification and Accreditation

The service provider shall provide an information assurance plan that shows how the service provider will comply with information assurance requirements. The service provider shall deliver secure, certified systems with all documentation necessary to accredit the system for operation on DoD Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) and/or SIPRNET networks. The service provider shall ensure compliance with FISMA via DoD Certification and Accreditation (CA) process for systems and the software certification process as defined by the iEHR software assurance policy for software and web applications. While final CA of the developed systems are the responsibility of the government, the service provider shall modify and/or develop systems with information assurance considerations integrated into the design of the software and system architecture. Knowledge of the DoD Information Assurance Certification and Accreditation Process (DIACAP)/National Institute of Standards and Technology (NIST) procedures is required.

5.2.2 DoD Information Assurance Policies

The service provider shall comply with fundamental DoD information assurance policy including:

- DoD Directive 8570.1, *Information Assurance Training, Certification, and Workforce Management*, certified current as of April 23, 2007

- DoD Directive 8500.01, *Information Assurance*, certified current as of April 23, 2007
- DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003
- DoD Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process* (DIACAP), November 28, 2007

5.2.3 Information Assurance

The contractor shall conform to NSTISSP No 11. National policy governing the acquisition of IA and IA-enabled technology products as of July 1, 2002 must be evaluated/validation by International Common Criteria Mutual Recognition (CCMR), NIAP Evaluation and Validation Program (CCEVS), NIST FIFPS validation program. All GOTS IA or IA enabled products must be evaluated by NSA or an NSA approved process. (Guidance DOD Directive (DODD) 8500.1– October 24, 2002, DOD Instruction (DODI) 85002– February 12, 2003).

IA Mitigation
The contractor shall work with the integrator to implement IA mitigation strategies include security updates, service packs, and changes to operating procedures as physical and cyber vulnerabilities are detected. Operating system, routers, servers, development platforms and the application being delivered to the Government shall be in compliance with all known applicable DoD Computer Emergency Response Team (DoD-CERT) alert, bulletin, and technical advisory notices published during the past 36 months.

IA Mitigation Strategies Applied
During product development for the Government, the contractor shall ensure that all IA mitigation strategies have been applied to the development environment prior to any Government data being loaded onto any assets or SW for testing or delivery.

The contractor shall maintain any development environments in accordance with DoD TMA and VA IA best practices and operational requirements.

Request for Waiver
A request for a waiver to the CA requirements may be submitted for temporary testing Interim Authority to Test (IATT), with deidentified data for usual circumstances. An IATT request must be submitted, in writing, by the contractor to the COTR. The waiver request must include mitigation strategies that ensure that adequate protection measures and security controls are in place (e.g. air gapping a testing network). The contractor shall provide support to the Government for completion and submission of an IATT plan where applicable.

6.0 Additional Information and Requirements

6.1 Legacy Reach-back Strategy

During transition from the DoD/VA legacy enterprise, iEHR will maintain a significant and critical dependence on existing healthcare applications, services, and repositories. The iEHR enterprise strategy for legacy interaction includes the use of Virtual Patient Record (VPR) services which shall serve as the authoritative source of patient healthcare record information for the enterprise. This capability will be responsible for managing the interaction with both new and legacy repositories going forward and includes the data federation, persistence, and semantic translation strategy required for legacy system interaction. As such, any iEHR application component or service which intends to interact with a given patient record (Search/CRUD activity) shall exclusively use the iEHR VPR services to do so. This is inclusive of any inter-domain patient record data which must be communicated across component, service, or system boundaries.

Similarly for orders management, iEHR Computerized Provider Order Entry (CPOE) services will also serve as the authoritative service set for creating and managing orders, result sets, and related order status. This service is responsible for both syntactic and semantic interoperability with both legacy and ancillary fulfillment/execution systems. As such, any iEHR application component or service which intends to perform order history, entry, change, status, or results management (Search/CRUD activity) shall exclusively use the iEHR CPOE services to do so. This is inclusive of any inter-domain orders (e.g. ancillary to ancillary) that must be communicated across component, service, or system boundaries.

Semantic interoperability shall be required to adhere to the iEHR CIIF mandated data ontologies for natively at all user interfaces and at component and system boundaries. The VPR and CPOE services shall translate, as necessary, to specific legacy system interfaces and repositories. Although these iEHR services are considered authoritative and mandatory for all interactions with patient records and orders, all system components and services shall be required to perform interoperability testing with the VPR as well as detailed regression testing against the legacy systems, including Community Health Centers Project (CHCS), Armed Forces Health Longitudinal Technology Application (AFHLTA) (including the CDR), Essentris, Veterans Health Information Systems and Technology Architecture (VistA), Computerized Patient Record System (CPRS), and the Health Data Repository (HDR)/Corporate Data Warehouse (CDW). Regression issues shall be reported to the iEHR IPO for resolution.

6.2 Legacy Re-use Strategy

There are numerous DoD and VA systems that currently provide support to the clinical and functional community business processes. In order to migrate systems in a planned and repeatable manner, a good understanding of the existing systems followed by an understanding of the ultimate end-state and interim architectures is required. It is also important to have visibility into the overall enterprise work space to ensure business continuity and collaboration rather than tackling system migration from a *silo* perspective. Transition Application Planning (TAP) is the methodology that is currently being used to identify which legacy programs, projects and initiatives can be shut off and/or migrated to the future state iEHR based upon the effectiveness of the application relevant to the business process, as well as the technical maturity of the application.

Through the TAP methodology, a large amount of legacy system data, including business processes, requirements, existing interfaces, business logic, data objects, software/hardware, and funding profiles are being collected, related, and leveraged to determine the most optimal sequence to migrate and/or retire legacy systems as the iEHR architecture and new capabilities are realized. Based on the iterative approach being used, prospective vendors must understand the current interfaces and technical requirements resident within the legacy systems as there will be a transition period where both legacy and new capabilities will be maintained until fully transitioned to the new capability.

Interfaces, protocols and systems currently in place, as related to the lab, pharmacy and immunizations capabilities are included within the architecture and standards compliance framework, and should be well understood by the prospective vendor. Additionally, as the TAP process is iterative in nature, the transition plan will be provided to potential contenders for understanding as available.

6.3 Low Com/No Com/Sync/Low IT Connectivity

Prospective vendors should be aware that the DoD has a requirement to provide a messaging service to the deployed applications, allowing electronic health records and other medical information to transmit from the theater of operations and low connectivity rural sites to home-based repositories. Current home-based repositories include the medical situational awareness in the theater, the theater medical data store and the CDR.

6.4 Systems Engineering Plan (SEP)

The Capstone SEP will guide the technical strategy of the joint DOD/VA iEHR program and map key acquisition Milestone (MS) events and deliverables to specific engineering activities. The Capstone SEP includes timing, conduct, and success criteria of technical reviews and efforts throughout the system life cycle.

The Capstone SEP describes the following systems engineering activities to be implemented across the program:

- Implementing Shared Agreements (Section 2.2)
- Implementing Technical Certifications (Section 2.3)
- Engineering Resources and Cost/Schedule Reporting (Section 3.2)
- Engineering and Integration Risk Management (Section 3.3)
- Managing Technical Performance Measures and Metrics (Section 3.7)
- Implementing the Engineering Approach (Section 3.8)
- Requirements Development and Change Process (Section 4.3)
- Performing Technical Reviews (Section 4.4)
- Performing Configuration Management (Section 4.5)
- Compliance with Design Considerations (Section 4.6)
- Implementing Agile practices and principles (4.7Appendix H)

6.5 Program Protection Plan (PPP)

TBD

6.6 Testing

6.6.1 Software Development Testing

- The number of tests performed and associated with the monthly cost and effort

- The location of the tests
- Staffing composition for the tests
- Development/requirements effort for the tests
- The number of defects identified and corrected as a result of testing
- Hardware configuration and procurement
- Level of end-user involvement in Early Operational Assessments (EOAs) and other equivalent activities. (Claiming that the use of former/retired individuals with recent experience in any of the tasks in lieu of scheduling activities with current end-users will be assessed as non-responsive to this Performance Work Statement (PWS)

6.7 System Development Plan

The plan outlines the incorporation of potential active duty end-users into the development process through EOAs or other equivalent activities. Claims including former/retired individuals with recent experience in any of the tasks, in lieu of scheduling activities with current end-users, will be assessed as non-responsive to this PWS.

6.7.1 Code Quality Checking

The contractor shall conduct Software Code Quality Checking (SCQC) throughout the development and testing phases of the project. The Government defines *SCQC* as a scan of the source code, executables, and related artifacts, e.g., documentation, to ensure that the system under development can continue with development, demonstration, and test, and can meet the stated performance, maintainability, and usability requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.

SCQC encompasses the use of static code analysis, static security analysis, dynamic code analysis, dynamic security analysis and architecture analysis and is usually performed using automated tools. The Government further defines the following terms:

- Static analysis is the analysis of computer software and related documentation that is performed without actually executing programs built from the software
- Static security analysis is the analysis of computer software that is performed without actually executing programs to detect and report weaknesses that can lead to security vulnerabilities
- Dynamic program analysis is the analysis of computer software and related documentation that is performed by executing programs built from that software on a real or virtual processor
- Dynamic security analysis is the analysis of computer software that is performed by executing programs to detect and report weaknesses that can lead to security vulnerabilities
- Architectural analysis may be supported by automated tools but are usually conducted by manual walk-through of documentation and visual inspection of the code

The Government will identify to the contractor the tools and methods the Government intends to use to conduct independent SCQC. Changes to the Government tool set, methods and criteria will be provided to the contractor with 90 days' notice.

The contractor shall report SCQC results periodically (periodicity to be negotiated with the contractor after contract award) using a defect removal efficiency matrix.

The Government will conduct its own independent SCQC inspection of the system under development up to three times during the development of the system. This may consist of over-the-shoulder testing at the contractor's facility or at the Government's SCQC facility. The contractor shall make available to the independent SCQC team the following artifacts in their current state at the time of request regardless of the method used:

- Source code and all design time libraries and licenses (static analysis)
- Executable code and libraries (dynamic analysis)
- Application configuration artifacts
- System Design Documents (SDD)
- System Sub-System Specification (SSS)
- System Sub-System Design Document (SSDD)
- System Security Authorization Agreement (SSAA)
- Interface Control Document (ICD)
- Database Design Document (DBDD)
- Test cases (dynamic analysis)
- Other artifacts proposed by the contractor

The Government's assessment of the contractor's code will reported in both the number and types of code quality and security vulnerabilities found as well as the *technical debt* or level of effort required to correct the defects.

6.7.2 Software Reviews and Scans

The service provider shall write software code (development or maintenance) in a secure fashion. At a minimum, the service provider shall perform the following reviews and scans to mitigate vulnerabilities to the maximum extent possible.

6.7.3 Code Reviews

The service provider shall conduct code reviews at an interval no less than once each calendar month. These code reviews shall be conducted and recorded as required by information assurance controls. The results of code review shall be documented and made available to the government.

6.7.4 Fortify Scans

Hewlett Packard Fortify is a code validation program that scans source code for known security vulnerabilities. The government will provide Fortify licenses unless specifically addressed otherwise in the task order.   The service provider shall use Fortify to scan code and identify vulnerabilities.

6.7.5 Software Vulnerability

The service provider shall deliver code with zero high and zero critical vulnerabilities identified by Fortify scans or other IA controls. The service provider shall provide risk assessment reports on any medium or low level vulnerabilities. This applies to all newly developed code. Applicability to previously written code will be addressed in the task order.

6.7.6 Security Technical Implementation Guide (STIG) Reviews

Reviews of all DISA Security Technical Implementation Guides (STIGs) that are applicable to task order software are required.   STIG reviews shall be documented and delivered to the government prior to the start of development on the task and thereafter on a yearly basis.

External References:

Software Assurance Pocket Guide Series: *Acquisition for Outsourcing*, Vol. 1 v1.1 July 31, 2009.

Software Assurance Pocket Guide Series: *Due Diligence*, Vol. 2 V1.2.

Both found at:

https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html

6.7.7 Testing

At the conclusion of system development, the contractor shall conduct a formal Development Integration Test (DIT). The contractor shall coordinate all formal test activities with the Government. Under no circumstances shall the contractor commit Government resources to a test event or test schedule prior to Government approval.

For each DIT the contractor shall develop a test plan specifically addressing the test objectives, test approach, test environment, success criteria, participant roles and responsibilities, documentation requirements, schedule and other items as identified in the Institute of Electrical and Electronics Engineers (IEEE) standard.

For each test, the contractor shall also develop test procedures that identify discrete events to be accomplished and actions and processes to be followed in the test activity. All functions to be tested shall be tied directly to the Requirements Traceability Matrix (RTM) and approved system design. Test procedures shall ensure that any new or changed interface is fully tested.

The contractor shall allow the Government and its representative to observe the installation of the software in contractor’s development environment.

The contractor shall resolve discrepancies and problems found during DIT prior to official release of the final software product to the Government. Upon the contractor’s determination that DIT has been successfully completed, they shall document the results in a test report. The report shall contain a detailed summary of test events, test findings, action items, and recommendations.

In certain circumstances such as a compressed delivery schedules, environmental limitations, or when an early look at the integrated product is necessary, the contractor shall allow Government and IVV agents to view the DIT in an over-the-shoulder review or allow them to test along with the contractor in a shoulder-to shoulder test. This type of testing shall only be conducted with prior approved of the Government.

Fifteen working days prior to TRR1, the Government shall require the contractor to test the installation of the application in the Government's test environment with DTE oversight to ensure the application successfully installs. This is in addition to SCQC testing and DIT inspections discussed in previous sections.

In addition the Government has the right to conduct *smoke* testing of the application and utilize the results in a preliminary user satisfaction survey. The contractor shall develop a smoke test plan that contains the following test scenarios that can be executed during smoke testing:

- Installation
- Validation of use cases
- Create, read, update, delete (CRUD) of data management
- Checks on Interfaces

- Roles and privileges
- Usability

Results of both installation and smoke shall be utilized to determine whether the Government will pass or fail TRR1. If the contractor is unable to install and pass the smoke test within the timeframe agreed upon by the contractor and the Government, the Government will not allow the contractor to conduct TRR1.

The Government will fail the SIT test event if the software cannot be installed utilizing Installation instructions provided the contractor and within the timeframe agreed upon by the contractor and the Government.

At the conclusion of DIT, the contractor shall conduct or support a Test Readiness Review (TRR) for the Government in order to present findings and to turn the developed function over to Configuration Management (CM) for subsequent Government testing. The contractor shall prepare the meeting agenda, coordinate meeting invitations, and present final versions of all system documentation at the TRR. In addition, all tool(s) and/or emulator(s) developed by the contractor specifically to test interfaces as a result of this development effort and associated documentation shall be delivered to the Government for use in Government testing.

After completion of the TRR and upon Government approval, the contractor shall support formal Government software testing. Test events may include System Integration Testing (SIT), System Qualification Testing (SQT), System Acceptance Testing (SAT), alpha/beta testing, and Operational Test and Evaluation (OTE).

The contractor shall conduct a Production Review (PR) following the successful completion of System Integration Testing in order to present the final results to the Government. The contractor shall present the final version of all system documentation at the PR. The contractor shall also ensure that an agenda and minutes for the PR are provided to all participants.

Contractor support may include providing on-demand access to various systems and facilities, real-time availability of engineering staff to support trouble-shooting, explaining nuances of system design, assisting in the setup of interface emulator tools, and performing quick fixes. In addition, the contractor shall participate in daily status meetings and end of test meetings and shall address test issues and problems found.

The table below describes error severity levels and is extracted from Joint Medical Information Systems (JMIS) Office Policy Memorandum #: 5.2.06, Subject: Test and Evaluation Severity and Category Code Guidelines dated March 31, 2005, which applies.

SevLvl Defect	Description
1	a. Prevents the accomplishment of an essential capability b. Jeopardizes the safety, security, or other requirements designated *Critical* c. Causes loss of a patient's life or seriously degrades the overall quality of a patient's health
2	a. Adversely affects the accomplishment of an essential capability and no workaround is known b. Adversely affects performance, cost, or schedule risks to the project or to life cycle support of the system, and no workaround is known
3	a. Adversely affects the accomplishment of an essential capability but a workaround has been identified b. Severely affects performance, cost or schedule risks to the project or to life cycle support of the system, but a workaround has been identified
4	a. Results in user inconvenience or annoyance but does not affect a required or mission essential capability b. Results in inconvenience or annoyance for development or maintenance personnel but does not prevent the accomplishment of responsibilities
5	Any other defect

Software products tendered that include severity level 1, 2 or clusters of 3s defects will be returned to the contractor for remediation and retest. A comprehensive contractor test (with an accompanying test report) is required of all software each time it is offered to the Government.

6.7.8 Test Metrics

The contractor will also provide the following information:

a. The number of tests performed shall be reported monthly with MPR
b. The location of the tests
c. Staffing composition for the tests
d. Development/requirements effort for the tests
e. The number of defects found and corrected during each test cycle
f. Hardware configuration and procurement

6.7.9 Variable/Multiple Platforms

It is the intent of the iEHR major initiative to allow clinical iEHR applications to directly run on any platform without special preparation. The iEHR will utilize software written in an interpreted language or pre-compiled portable bytecode for which the interpreters or run-time packages are common or standard components of all platforms. This approach is consistent with the key principles outlined in the Draft U.S. Department of Veterans Affairs Enterprise Mobile Platform Strategy. The key principles of the VA Enterprise Mobile Platform Strategy include:

- Creating a customer-driven environment for the use of mobile technology for VA employees, Veterans, clinicians and service providers, dependents and annuitants. To achieve this outcome, an agile and dynamic governance process will be used to address risk, the needs of users, while simultaneously ensuring VA data security and integrity.
- VA Mobile Applications will be developed according to published VA standards. Mobile application certification considerations will include safety, fitness, security, privacy, engineering, human interface design, and Section 508 compliance.

- Service Discovery will be achieved by standing up the VA Mobile App Store (MAS).   Once the mobile applications are certified, they will be published into the VA Mobile App Store (MAS) under VA branding. The VA Mobile App Store (MAS) will address the need of enterprise mobile application discovery. The VA MAS will afford security protections in addition to managing and serving as the authorized source for VA mobile applications. The VA Mobile App Store will provide four fundamental service discovery capabilities: Inquiry, Publishing, Security, and Subscription.
- Entrance into the mobile development environment will have limited barriers, to allow for collaboration and standardization. The mobile development environment will be device agnostic, and mobile applications will be developed with the intent to operate on all mobile device platforms once provisioned. It is also expected that mobile application code be developed and documented in such a way as to allow for it to be re-used in addition to leveraging defined terminology standards, which would ultimately improve collaboration and documentation efforts.   Alignment with agile methodology and open source tools with a focus on ensured patient safety and the safety of VA data will be important to the mobile development environment.

APPENDIX A: REFERENCES

1.) IEHR BUSINESS NEEDS STATEMENT, JUNE 10, 2012

APPENDIX B: ASSOCIATED ARTIFACTS

B.2.0 iEHR Enterprise Architecture

- B.2.0.1 AV - All Viewpoint
  - AV-1 Overview and Summary
  - AV-2 Integrated Dictionary
- B.2.0.2 CV – Capability Viewpoint
  - CV-1 Capability Vision
  - CV-2 Capability Taxonomy
  - CV-3 Capability Phasing
  - CV-6 Capability to Operational Activity Mapping
  - CV-7 Capability to Services Mapping
- B.2.0.3 DIV – Data and Information Viewpoint
  - DIV-1 Conceptual Data Model
  - DIV-2 Logical Data Model
  - DIV-3 Physical Data Model
- B.2.0.4 OV – Operational Viewpoint
  - OV-1 Operational Concept Graphic
  - OV-2 Operational Resource Flow Description
  - OV-3 Operational Resource Flow Matrix
  - OV-4 Organizational Relationship Chart
  - OV-5 Operational Series Viewpoints
    - OV-5a Operational Activity Node Tree
    - OV-5b Operational Activity Model
  - OV-6 Series Viewpoints
    - OV-6a Operational Rules Model
    - OV-6b State Transition Description
    - OV-6c Event-Trace Description
- B.2.0.5 StdV – Standards Viewpoint
  - StdV-1 Standards Profile
  - StdV-2 Standards Forecast
- B.2.0.6 SV – Systems Viewpoint
  - SV-1 Systems Interface Description
  - SV-2 Systems Resource Flow Description
  - SV-4 Systems Functionality Description
  - SV-5 Operational Activity to Systems Function Traceability Matrix
  - SV-6 Systems Resource Flow Matrix
- B.2.0.7 SvcV – Services Viewpoint
  - SvcV-1 Services Context Description
  - SvcV-2 Services Resource Flow Description
  - SvcV-2 Services Resource Flow Description

SvcV-5 Operational Activity to Services Traceability Matrix
SvcV-6 Services Resource Flow Matrix
B.2.1 Architecture and Standards Compliance Criteria
B.2.2 Open API's and Common Interface Standards

B.3.0 Enabling Infrastructure Capabilities
B.3.1 Access
B.3.2 Identity Management
B.3.3 Network and Security
B.3.4 SSO CM
B.3.5 Virtualization
B.3.6 Common Information Interoperability Framework CIIF
B.3.7 Health Data Dictionary HDD and Custodial Agent CA
B.3.8 Virtual Lifetime Electronic Record VLER
B.3.9 SOA SOE ESB
B.3.10 Portal Framework
B.3.11 Presentation Layer (User Experience - UX)
B.3.12 Data Infrastructure
B.3.13 Development Testing Center (DTC) - Development and Test Environment (DTE)
B.3.13.1 Development
B.3.13.2 Development Integration Test (DIT)
B.3.13.3 Test
B.3.13.4 Software Integration Test (SIT)
B.3.13.5 Training and Demonstration

B.4.0 Clinical Requirements
B.4.1 Laboratory Capability
B.4.2 Pharmacy Capability
B.4.3 Immunization Capability
B.4.4 iEHR Certification - Meaningful Use
B.4.5 Healthcare End-User Usability
B.4.6 Patient Driven Care and Care Coordination
B.4.7 Cognitive Support - Knowledge Management - Clinical Decision Support
B.4.8 Business Intelligence / Analytics

B.5.0 Privacy Security and Info Assurance Requirements
B.5.1 Privacy and Security
B.5.2 Software and Info Assurance
B.5.2.1 Software Security Certificates and Accreditations
B.5.2.2 DoD IA Policies
B.5.2.3 Information Assurance

B.6.0 Additional Information and Requirements

- B.6.1 Legacy Reach-back Strategy
- B.6.2 Legacy Re-use Strategy
- B.6.3 Low Com No Com Sync Low IT Connectivity
- B.6.4 Systems Engineering Plan (SEP)
- B.6.5 Program Protection Plan (PPP)
- B.6.6 Testing
  - B.6.6.1 Software Development Testing
- B.6.7 System Development Plan
  - B.6.7.1 Code Quality Checking
  - B.6.7.2 Software Reviews and Scans
  - B.6.7.3 Code Reviews
  - B.6.7.4 Fortify Scans
  - B.6.7.5 Software Vulnerability
  - B.6.7.6 Security Technical Implementation Guide (STIG) Reviews
  - B.6.7.7 Testing
  - B.6.7.8 Test Metrics
  - B.6.7.9 Variable - Multiple Platforms

*Representative artifacts available at www.tricare.mil/iEHR then click on **Vendor Information** in the left column.*

APPENDIX C: ACRONYMS

A	
API	Application Programming Interface
AIS	Automated Information System
B	
	Business Associate Agreement
C	
C&A	Certification and Accreditation
CA	Custodial Agent
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMR	Common Criteria Mutual Recognition
CDA	Clinical Document Architecture
CDD	Certificate of Data Destruction
CDL	Common Development Library
CDS	Clinical Decision Support
CDW	Corporate Data Warehouse
CFR	Code of Federal Regulations
CHCS	Community Health Centers Project
CIIF	Common Information Interoperability Framework
CM	Configuration Management
COTR	Contracting Officer's Technical Representative
COTS	Commercial off the Shelf
CPGs	Clinical Practice Guidelines
CPOE	Computerized Provider Order Entry
CPRS	Computerized Patient Record System
CQMs	Clinical Quality Measures
CRUD	Create, Read, Update and Delete
D	
DBDD	Database Design Document
DHHS	Department of Health and Human Services
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DIT	Development Integration Test
DoD	Department of Defense
DoD-CERT	DoD Computer Emergency Response Team
DoDAF	DoD Architecture Framework
DSA	Data Sharing Agreement
DTC	Development Test Center
DTE	Developmental Test and Evaluation

DTE	Development and Test Environment

E

EC2	Elastic Compute Cloud
EOAs	Early Operational Assessments
ESB	Enterprise Service Bus

F

FDCCI	Federal Data Center Consolidation Initiative
FDR	Federated Data Repository
FHP	Force Health Protection
FIM	Functional Independence Measure
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act

G

GFI	Government Furnished Information
GOTS	Government Off the Shelf
GUI	Graphic User Interface

H

HDD	Health Data Dictionary
HDR	Health Data Repository
HIT	Health Information Technology
HITPC	HIT Policy
HITSC	HIT Standards

I

IA	Information Assurance
IATT	Interim Authority to Test
ICD	Interface Control Document
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
iEHR	interagency Electronic Health Record
IOS	International Organization for Standardization
IPO	Interagency Program Office
IT	Information Technology

J

JMIS	Joint Medical Information Systems

L

LOINC	Logical Observation Identifiers Names and Codes

M

MHS	Military Health System
MTF	Military Treatment Facility

N

NCQA	National Committee for Quality Assurance
NIAP	National Information Assurance Partnership
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NwHIN	Nationwide Health Information Network

O

OMB	Office of Management and Budget
ONC	Office of National Coordinator
OTE	Operational Test and Evaluation

P

PCMH	Patient Centered Medical Home
PHQ-9	Patient Health Questionnaire
PII	Personally Identifiable Information
PIM	Patient Identity Management
PIV	Personal Identification Verification
PR	Production Review
PROMIS	Patient Reported Outcomes Measurement Information System
PWS	Performance Work Statement

R

RACE	Rapid Access Computing Environment
RFB	Look-Feel-Behavior
RTM	Requirements Traceability Matrix

S

SAT	System Acceptance Testing
SCQC	Software Code Quality Checking
SDD	System Design Document
SDK	Software Development Toolkit
SECDEF	Secretary of Defense
SECVA	Secretary of Veterans Affairs
SEP	System Engineering Plan

SIPRNET	Secret Internet Protocol Router Network
SIT	Software Integration Test
SNOMED	Systematic Nomenclature of Medicine
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOE	Service Oriented Enterprise
SOI	Service Oriented Infrastructure
SOP	Standard Operating Procedure
SPIIHI	Standards for Privacy of Individually Identifiable Health Information
SQT	System Qualification Testing
SSAA	System Security Authorization Agreement
SSDD	System Sub -System Design Document
SSO/CM	Single Sign-on with Context Management
SSS	System Sub-System Specification
STIG	Standard Technical Implementation Guide

T

TAP	Transition Application Planning
TMA	Tricare Management Activity
TRR	Test Readiness Review

U

UCD	User-Centered Design

V

VA	Department of Veterans Affairs
VISTA	Veterans Health Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VPR	Virtual Patient Record
VR-12	Veterans Rand 12

W

WS-I	Web Services Interoperability
WSDL	Web Services Description Language

X

XML	Extensible Markup Language
XSD	XML Schema DefinitionX